REMARKS

I. INTRODUCTION

Claims 1-18 are pending in the present application. Applicants thankfully acknowledge the Examiner's indication that claim 18 would be allowed if rewritten. However, in view of the following remarks, it is respectfully submitted that all of the presently pending claims are allowable.

II. THE 35 U.S.C. § 102(b) REJECTIONS SHOULD BE WITHDRAWN

Claims 1-5 stand rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,991,408 to Pearson et al. ("the Pearson reference"). (See 5/4/05 Office Action, p. 2).

The Pearson reference describes a system for processing a user which includes a sensor 401 connected to a computer system 404. The computer system 404 includes an interface 406 connected to a processor 408 which is connected to a memory 412. (See the Pearson reference, col. 7, lines 30-49). The memory 412 stores a representation of a user's fingerprint 416 and an instance of a problem 418. (Id. at col. 7, lines 49-51). The representation 416 is read from the sensor 401 into the memory 412, encoded, and checked against the instance of the problem 418 to determine if the representation 416 solves the instance of the problem 418. (Id. at col. 7, line 64 - col. 8, line 44). If a solution to the instance of the problem 418 is found, a private key may be generated from the solution and used to decrypt information that was encrypted using a public key generated from a representation of the user's fingerprint 116 during an enrollment process 200. (Id. at col. 9, lines 34-38).

Claim 1 of the present invention recites a semiconductor device for securely controlling access to cryptographic processing of data which comprises "a semiconductor package" and "a *cryptographic processor* disposed in the semiconductor package, the processor including a biometric data capture device operative to acquire biometric data associated with a predetermined biometric characteristic of a user and *store the biometric data as a biometric key,* and an encryption/decryption circuit operative to perform encryption or decryption on input data utilizing said biometric key." The specification of the present invention distinguishes the cryptographic processor from general processors. As shown in Fig. 1, a system according to the present invention utilizes a cryptographic module 10 in addition to the processor 15. (See Specification, Fig. 1). The specification states that "the processor 15 cannot access the unencrypted biometric data nor can it access the key used to encrypt the data," and that one reason for doing so is because "the processor can be compromised by a malicious program" and therefore, "the sensor data must be secured independently of the main CPU." (Id. at p. 15). Thus, the cryptographic processor has access to the unencrypted biometric data and the biometric key, whereas the general processor does not.

In contrast, the Pearson reference states that the computer system 404 may be any type of computer system, and the processor 408 may be any type of processor. (See the Pearson reference, col. 7, lines 52-60). Thus, both the computer system 404 and the processor 408 are conventional devices which are general-purpose, rather than specialized for any specific task. However, even if the processor 408 were capable of performing the functions associated with the cryptographic processor of the present invention, the processor 408 could not be both a general processor and a cryptographic processor, since this would be in direct contrast to the teachings of the present invention. Thus, it is respectfully submitted that the processor 408 is not a "cryptographic processor."

Furthermore, the Pearson reference does not disclose the storing of biometric keys. According to the Pearson reference, when the user first enrolls into the system, a public key is generated from the user's biometric data for encrypting information. (Id. at col. 6, lines 45-58).

The public key is then transmitted through an input-output line 102. (Id. at col. 7, lines 23-29). No indication is given that the public key is stored on the processor 408, or anywhere else on the computer 404. Similarly, the private key is not stored, but is instead generated each time the representation of the user's fingerprint 416 successfully solves the instance of the problem 418. The representation of the user's fingerprint 416 and the instance of the problem 418 are not biometric keys, since they are not utilized to encrypt and decrypt information. Thus, the processor 408 does not "store the biometric data as a biometric key." Therefore, it is respectfully submitted that the Pearson reference does not disclose or suggest "a cryptographic processor" which "store[s] the biometric data as a biometric key," as recited in claim 1.

It is respectfully submitted that claim 1 is not anticipated by the Pearson reference for the reasons discussed above and that this rejection should be withdrawn. Because claims 2-5 depend from and, therefore, include all of the limitations of claim 1, it is respectfully submitted that these claims are also allowable.

III. THE 35 U.S.C. § 103(a) REJECTIONS SHOULD BE WITHDRAWN

Claims 6-10 stand rejected under 35 U.S.C. §103(a) as being unpatentable over the Pearson reference in view of U.S. Patent No. 6,219,793 to Li et al. ("the Li reference"). (See 5/4/05 Office Action, p. 3).

Independent claim 6 recites "a *cryptographic processor* disposed in a single semiconductor package, the processor including a biometric data capture device contained in the semiconductor package to capture biometric data associated with a predetermined biometric characteristic of a user and *store the biometric data as a biometric key*." This limitation is similar to the recitation described above with reference to claim 1. Thus, for the same reasons as described above, the Pearson reference neither teaches nor suggests this recitation of claim 6. The Li reference fails to cure this deficiency of the Pearson reference. Therefore, it is

respectfully submitted that neither the Pearson reference nor the Li reference, either alone or in combination, teaches or suggests "a cryptographic processor disposed in a single semiconductor package, the processor including a biometric data capture device contained in the semiconductor package to capture biometric data associated with a predetermined biometric characteristic of a user and store the biometric data as a biometric key," as recited in claim 6. Thus, it is respectfully submitted that claim 6 and claims 7-10, which depend therefrom, are allowable.

Claims 11-17 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over the Pearson reference in view of U.S. Patent No. 6,484,260 to Scott et al. ("the Scott reference"). (See 5/4/05 Office Action, p. 4).

Independent claim 11 recites "a mobile computer including a *cryptographic processor*" and "a *stored encrypted biometric key* in said cryptographic processor." This limitation is similar to the recitation described above with reference to claim 1. Thus, for the same reasons as described above, the Pearson reference neither teaches nor suggests this recitation of claim 6. The Scott reference fails to cure this deficiency of the Pearson reference. Therefore, it is respectfully submitted that neither the Pearson reference nor the Scott reference, either alone or in combination, teaches or suggests "a stored encrypted biometric key in said cryptographic processor," as recited in claim 11. Thus, it is respectfully submitted that claim 11 and claims 12-17, which depend therefrom, are allowable.

Because claim 18 depends from and, therefore, includes all of the limitations of claim 11, it is respectfully submitted that this claim is also allowable for the reasons stated above with reference to claim 11.

CONCLUSION

In light of the foregoing, the applicants respectfully submit that all of the pending claims are in condition for allowance. All issues raised by the Examiner have been addressed, an early and favorable action on the merits is earnestly solicited.

Respectfully submitted,

Dated: August 4, 2005

By: _____
Oleg F. Kaplun (Reg. No. 45,559)

Fay Kaplun & Marcin, LLP
150 Broadway, Suite 702
New York, NY 10038
Tel: (212) 619-6000
Fax: (212) 619-0276